AF/ZW

Attorney's Docket No. 3361-011773

SECOND AMENDED APPEAL BRIEF TRANSMITTAL LETTER

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application No.: 10/055,407 Filing Date: 01/23/2002

Examiner: Arrienne M. Lezak Art Unit: 2143

Invention: **"METHOD FOR MANAGING COMPUTER NETWORK ACCESS"**

Transmitted herewith is a Second Amended Appeal Brief Under 37 C.F.R. § 41.37 in the above-identified application.

- x Small Entity Status is/has been asserted for this application under 37 CFR 1.27.
- ___ A verified statement to establish small entity status under 37 CFR 1.27 is enclosed.
- x No additional fee is required.
- ___ The fee has been calculated as shown below:

	No. of Claims After Amendment	Highest No. Previously Paid For	Present Extra	Small Entity Rate	Non-Small Entity Rate	Charge
Total	23	23	0	x $ 25.00	x $ 50.00	$ 0
Indep.	3	3	0	x $100.00	x $200.00	$ 0
First Presentation of Multiple Dependent Claim/s				+ $180.00	+ $360.00	$ 0
				TOTAL ADDITIONAL FEE		$ 0

- ___ A check in the amount of $ ___ is enclosed to cover the additional.
- ___ A check in the amount of $___ is enclosed for a __ month Petition for Extension of Time.
- x The Commissioner is hereby authorized to charge payment of the following fees associated with this communication to Deposit Account No. 23-0650. Please refund any overpayment to Deposit Account No. 23-0650. An original and two copies of this sheet are enclosed.
- x Any additional filing fees required under 37 CFR 1.16.
- x Any patent application processing fees under 37 CFR 1.17.

February 1, 2007
Date

By _____
William H. Logsdon
Registration No. 22,132
Attorney for Applicants
700 Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219
Telephone: (412) 471-8815
Facsimile: (412) 471-4094
E-mail webblaw@webblaw.com

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on February 1, 2007.

Deborah L. Hartmann
(Name of Person Mailing Paper)

Deborah L. Hartmann 02/01/2007
Signature Date

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.	:	10/055,407	Confirmation No.: 7264
Applicants	:	David A. Fertell et al.	
Filed	:	January 23, 2002	
Title	:	**METHOD FOR MANAGING COMPUTER NETWORK ACCESS**	
Art Unit	:	2143	
Examiner	:	Arrienne M. Lezak	
Customer No.	:	28289	

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

LETTER

Sir:

In response to the Notification Of Non-Compliant Appeal Brief (37 CFR 41.37), dated January 26, 2007, Applicants submit the accompanying Second Amended Appeal Brief Under 37 C.F.R. § 41.37.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to Commissioner for Patent, P.O. Box 1450, Alexandria, VA 22313-1450 on February 1, 2007.

Deborah L. Hartmann
(Name of Person Mailing Paper)

Deborah L. Hartmann 02/01/2007
Signature Date

It is believed that all the matters raised in the Notification have been addressed in the attached Second Amended Appeal Brief which is believed to be fully compliant with the requirements of 37 C.F.R. § 41.37.

Applicants respectfully request that the final rejection on the merits be reversed and a Notice of Allowance issued.

Respectfully submitted,

THE WEBB LAW FIRM

By _____

William H. Logsdon
Registration No. 22,132
Attorney for Applicants
700 Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219
Telephone: 412-471-8815
Facsimile: 412-471-4094
E-Mail: webblaw@webblaw.com

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.	:	10/055,407	Confirmation No.: 7264
Applicants	:	David A. Fertell et al.	
Filed	:	January 23, 2002	
Title	:	**METHOD FOR MANAGING COMPUTER NETWORK ACCESS**	
Art Unit	:	2143	
Examiner	:	Arrienne M. Lezak	
Customer No.	:	28289	

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SECOND AMENDED APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Dear Sir:

(I) REAL PARTY OF INTEREST

The real party of interest in this Appeal is Pearl Software, Inc., 64 East Uwchlan Avenue, Suite 230, Exton, Pennsylvania.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to Commissioner for Patent, P.O. Box 1450, Alexandria, VA 22313-1450 on February 1, 2007.

Deborah L. Hartmann
(Name of Person Mailing Paper)

Deborah L. Hartmann 02/01/2007
Signature Date

(II) RELATED APPEALS AND INTERFERENCES

None.

(III) STATUS OF THE CLAIMS

Claims 1-23 are pending. Claims 1-23 are appealed.

(IV) STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final rejection.

(V) SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 generally recites a method for controlling computer network access. The method includes (a) initiating at a client computer 1 a first communication session 100 at a first network address (paragraph 0052, lines 3-7, and Fig. 1); (b) receiving at the client computer 1 via the first communication 100 a second network address (paragraph 0052, lines 8-11); (c) initiating at the client computer 1 a second communication session 102 at the second network address (paragraph 0052, lines 12-15); (d) receiving at the client computer 1 via the second communication session 102 an access configuration (paragraph 0045 and paragraph 0053, lines 1-5) including a control setting for at least one communication protocol capable of being utilized (paragraph 0054 through paragraph 0057, and Fig. 2) during a third communication session 104; (e) instantiating on the client computer 1 a process which initiates a third communication session 104 at a third network address (paragraph 0055, lines 1-3); and (f) in connection with the third communication session 104, controlling the conveyance of data either to or from the process instantiated on the client computer 1 based on the control setting for the one communication protocol (paragraph 0055, lines 3-21).

Claim 7 depends from claim 1 and includes at least one of the following steps: after (b), terminating the first communication session 100 (paragraph 0053, lines 1 and 2); and/or after step (d), terminating the second communication session 102 (paragraph 0075, lines 1-5).

Claim 8 depends from claim 1 and includes the further steps of: transmitting from the client computer 1 via the second communication session 102 a request to receive another access configuration including a control setting for the one communication protocol (paragraphs 11 and 70); receiving at the client computer 1 via the second communication session 102 the other access configuration (paragraphs 11 and 70); and performing step (f) based on the control setting included in the other access configuration (paragraph 0011, lines 4-6).

Claim 10 depends from claim 9 and includes the further step of transferring at least part of the conveyed data to the second network address via the second communication session 102 (paragraph 0057, lines 1-4).

Independent claim 13 generally recites a method for controlling computer network access that includes the steps of: (a) storing at a client computer 1 a first network address 100 (paragraph 0052, lines 5-8, Fig. 1); (b) initiating a first communication session between the client computer 1 and a first server computer 2 at the first network address 100 (paragraph 0052, lines 5-7, Fig. 1); (c) receiving at the client computer 1 from the first server computer 2 via the first communication session a second network address 102 or 102N (paragraph 0052, lines 8-11, Fig. 1); (d) initiating a second communication session between the client computer 1 and a second server computer 2 or 5 at the second network address 102 or 102N (paragraph 0052, lines 12-17, Fig. 1); (e) receiving at the client computer 1 from the second server computer 102 or 102N an access configuration (paragraph 0053, lines 1-5, Fig. 1) including a control setting for at least one communication protocol capable of being utilized during a third communication session (paragraphs 54-57); (f) instantiating on the client computer 1 concurrent with the second communication session a process which initiates a third communication session 104 between the

client computer 1 and a remote computer 3 at a third network address (paragraph 0055, lines 1-3, Fig. 1); and (g) in connection with the third communication session 104, controlling data conveyed at least one of (i) to and (ii) from the instantiated process on the client computer 1 based on the control setting for the one communication protocol (paragraph 0055, lines 3-21, Figs. 1-3a).

Claim 15 depends from claim 13 and includes at least one of the following steps: after step (c) the step of terminating the first communication session 100 (paragraph 0053, lines 1 and 2); and/or after step (e), terminating the second communication session 102 (paragraph 0075, lines 1-5).

Claim 18 depends from claim 13 and includes the further steps of: initiating at the client computer 1 via the second communication session 102 a request to the second server computer 2 or 5 to transmit another access configuration (paragraphs 11 and 70); receiving at the client computer 1 from the second server computer 2 or 5 the other access configuration (paragraphs 11 and 70); and performing step (g) based on a control setting included in the other access configuration for the one communication protocol (paragraph 0011, lines 4-6).

Independent claim 22 recites a method of controlling computer network access comprising: (a) initiating a communication session 102 between a first computer 1 and a second computer 2 or 5 (paragraph 0052, lines 8-17); (b) receiving at the first computer 1 from the second computer 2 or 5 via the communication session 102 an access configuration including a control setting for at least one communication protocol (paragraph 0053, lines 1-5, Fig. 1); (c) monitoring data conveyed to or from a process running on the first computer 1 based on the control setting (paragraph 0055, lines 3 and 4); and (d) controlling the data conveyed to or from the process based on the control setting (paragraph 0055, lines 5-21).

Claim 23 depends from claim 22 and includes the further limitation that the process instantiates another computer communication session 104 (paragraph 0055, lines 1-3); and the conveyance of data is controlled in connection with the other communication session 104 (paragraph 0055, lines 3-21).

(VI) GROUND(S) OF REJECTION TO BE REVIEWED ON APPEAL

Are claims 1-23 obvious under 35 U.S.C. § 103(a) from the teachings of U.S. Patent No. 5,950,195 to Stockwell et al.[1]

(VII) ARGUMENT

In accordance with 37 C.F.R. § 41.37(c)(VII), it is respectfully requested that the patentability of each claim argued separately be considered separately.

Claim 1:

Claim 1 generally recites a method for controlling computer network access. The method includes initiating at a client computer a first communication session at a first network address and receiving at the client computer via the first communication session a second network address. A second communication session is initiated at the client computer at the second network address. The client computer receives via the second communication session an access configuration including a control setting for at least one communication protocol capable of being utilized during a third communication session. A process is instantiated on the client computer which initiates a third communication session at a third network address. In connection with the third communication session, the conveyance of data to or from the process instantiated on the client computer is controlled based on the control setting for the one communication protocol.

In rejecting independent claims 1, 13 and 22, the Examiner alleges, among other things, that column 5, line 17 through column 6, line 58; column 7, line 34 through column 8, line 37; and column 11, lines 6-32 of the Stockwell et al. patent disclose all the limitations of these

[1] In section 2 of the October 7, 2005 Office Action, claims 1-23 were rejected for obviousness from the teachings of U.S. Patent Publication No. US 2002/0169961 A1 to Stockwell et al. However, this publication is to Giles et al. In a telephone conversation on January 3, 2006, the Examiner confirmed that she had intended to reject the claims over U.S. Patent No. 5,950,195 to Stockwell et al.

claims.

In response to this rejection in the Response mailed January 9, 2006, Applicants argued as follows:

> In contrast, the Stockwell et al. patent discloses that an Access Control List (ACL) is managed by an acld deamon (acld 60) running in the kernel of a firewall 10/30 (see column 5, lines 36-37), which is used to regulate the flow of Internet connections from an internal network 26 to an external network 22 (see column 4, lines 29-31). The Stockwell et al. patent discloses, teaches and suggests that its firewall 10/30 is utilized to facilitate communication between undisclosed computers connected to the firewall via internal network 26 and external network 22. What is clear in the Stockwell et al. patent, however, is that the firewall 10/30 is not a client computer in the same sense as the client computer of the present invention configured for use by an end user.
>
> Assuming *arguendo*, the firewall disclosed in the Stockwell et al. patent is analogous to the client computer of claim 1, the Stockwell et al. patent does not disclose, teach or suggest a method having all the limitations of claim 1. Specifically, step (d) of claim 1 recites that the client computer receives an access configuration including a control setting for at least one communication protocol via a (second) communication session. In contrast, the Stockwell et al. patent discloses, teaches and suggests that acld 60 (synonymous to the access configuration of the present invention) always resides at the firewall (see column 7, lines 10-20). Specifically, to make an ACL check, an agent, such as proxy 50, server 52, login 54 or network access server 56 shown in Fig. 3, collects information about the nature of a connection, such as source and destination IP addresses. The agent places this information into a query list that contains all of the relevant information needed to make the ACL check. The agent then submits the query list to acld 60 and acld 60 searches for a rule that matches the query list and returns a reply list. This reply list includes either "allow" or "deny" to indicate if the connection should be accepted or rejected. Other values in the reply list are side effects that change the behavior of the agent.
>
> As can be seen, the access configuration upon which a decision is made whether to allow or deny access resides in acld 60. No agent contains information upon which to base a decision whether to allow or deny access. Rather, only the "allow" or "deny" indicator is provided to the agent by acld 60. In other words, the Stockwell et al. patent discloses, teaches and suggests that the ACL rules reside

permanently in acld 60. Accordingly, the Stockwell et al. patent cannot disclose, teach or suggest the limitations of claim 1, step (d), namely, that an access configuration including a control setting for at least one communication protocol is received at the client computer via a (second) communication session.

Moreover, the Stockwell et al. patent does not disclose the limitations of claim 1, step (f), namely, controlling the conveyance of data to or from a process that initiates a third communication session at a third network address based on the control settings included in the access configuration received at the computer via the second communication session. The differences between the present invention and the teachings of the Stockwell et al. patent in this regard are relatively straightforward. In the present invention, the client computer can attempt to access a specific IP address. Rules for this access attempt are checked at the client computer and a decision is made thereat whether to allow or deny access. No Internet traffic need traverse a firewall that may or may not be accessible to the client computer in order to make this decision. In contrast, in the Stockwell et al. patent, the same client computer would attempt a communication with a specific IP address through the disclosed firewall 10/30, which would determine whether to allow or deny access. Thus, as can be seen, the Stockwell et al. patent discloses a system wherein the decision to deny or allow access is made at a completely different location than the method claimed in claim 1.

Moreover, the Stockwell et al. patent does not disclose, teach or suggest a client computer utilizing multiple communication sessions, each of which is at a different network address. Rather, the Stockwell et al. patent discloses, teaches and suggests communications between internal processes of a firewall – not between different network addresses.

On page 4 of the Office Action, the Examiner admits that the Stockwell et al. patent "does not specifically enumerate a first, second and third communication session at a respective network address." The Examiner goes onto allege, however, that it would have been obvious to one of ordinary skill in the art at the time of the invention to use any number of multiple servers to perform a task - "In other words, within a network system comprising multiple servers and multiple layers of access control, Stockwell teaches secured access throughout the network as implemented on multiple machines wherein it would have been obvious to create multiple communication sessions for added security and improved performance purposes."

It is well established patent law that in order to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on Applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

As discussed above, the Stockwell et al. patent discloses, teaches and suggests communications between internal processes of a firewall - not between different network addresses. Accordingly, if anything, the Stockwell et al. patent teaches away from a single client computer utilizing first, second and third communication sessions at first, second and third network addresses in the manner disclosed in claim 1. Hence, the Stockwell et al. patent does not meet the first prong of the above test.

Moreover, it is respectfully submitted that the Examiner's allegation on page 4 of the Office Action fails to meet the final prong of the test, namely, that the prior art reference teaches and suggests all of the claim limitations. Assuming *arguendo* that in view of the Stockwell et al. patent, one skilled in the art would have used any number of multiple servers to perform authentication, access control or information acquisition (as alleged by the Examiner), the Examiner has not explained why one skilled in the art would have chosen the specific method claimed in claim 1 of the present application to perform this task. Indeed, the Examiner has not explained why one skilled in the art would use three communication sessions versus any number of communication sessions other than three. Accordingly, it is respectfully submitted that the Examiner has used impermissible hindsight to reject claim 1.

In the "Response to Arguments" section of the April 7, 2006 Office Action, the Examiner alleges that "Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made".

As can be seen from the foregoing quoted paragraphs of the January 9, 2006 Response, Applicants have clearly argued that the Stockwell et al. patent does not disclose, teach or suggest the limitations of step (d) of claim 1 or step (f) of claim 1. Moreover, Applicants have specifically argued that the Stockwell et al. patent does not contain the required suggestion or motivation to modify the teachings thereof in a manner that results in a method having all the limitations of claim 1. To this end, Applicants have argued that the Stockwell et al. patent teaches away from a single client computer utilizing first, second and third communication sessions at first, second and third network addresses in the manner disclosed in claim 1. Moreover, Applicants have clearly argued that the Stockwell et al. patent fails to teach and suggest all of the claim limitations, and that the Examiner has utilized impermissible hindsight to reject claim 1.

Accordingly, it cannot be legitimately argued that the Applicants' arguments in the January 9, 2006 Response do not comply with 37 CFR § 1.111(c).

In the "Response to Arguments" section of the April 7, 2006 Office Action, the Examiner argues:

> Regarding Applicant's argument that Stockwell does not teach receipt of access configuration at the client computer, Examiner respectfully disagrees. Specifically, Examiner notes that not only could the firewall taught by Stockwell be incorporated into a client computer, Stockwell further teaches an authentication means utilizing proxies and warders, Figs. 1-3; Col. 5, lines 53-67; & Col. 6, lines 1-67). Additionally, Stockwell teaches a user authentication means, (Col. 6, lines 8-27), as well as an authentication and redirection means, (Col. 8, lines 1-37 & Col. 11, lines 6-32), all of which clearly and obviously involve receipt of access configuration at a client computer.

In making the foregoing allegation, the Examiner alleges "all of which clearly and obviously involve receipt of access configuration at a client computer" (underline added). The Stockwell et al. patent discloses that firewalls 10 and 30 in Figs. 1 and 2, respectively, are used to regulate the flow of internet work connections from an internal to an external network. Since a client computer will typically reside either on the internal network or the external network, it

cannot legitimately be argued that firewalls 10 and 30 in the Stockwell et al. patent are incorporated into a client computer, as alleged by the Examiner. Moreover, there is no teaching or suggestion in the Stockwell et al. patent of a client computer having a firewall incorporated therein. Moreover, the mere fact that the Stockwell et al. patent discloses that firewall 10 and firewall 30 utilize proxies, warders and redirection means does not *per se* teach or suggest that the firewall taught by Stockwell et al. is incorporated into a client computer. If it were, the Examiner would not have speculated that the firewall of the Stockwell et al. patent "could" be incorporated into a client computer.

In the "Response to Arguments" section of the April 7, 2006 Office Action, the Examiner alleges:

> In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "client computer/mobile client access without traversing a firewall" and "the use of a common/single network address for all computer 1 session initiations without the use of a firewall") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

It is respectfully submitted that the Examiner has read the arguments presented in the January 9, 2006 Response out of context. Specifically, in the paragraph bridging pages 3 and 4 of this Response, Applicants' have argued "[r]ules for this access attempt are checked at the client computer and a decision is made thereat whether to allow or deny access. No internet access need traverse a firewall that may or may not be accessible to the client computer in order to make this decision."

When read in context, it can be seen that the sentence stating that no internet traffic need traverse a firewall is simply a sentence to contrast the present invention over the Stockwell et al. patent which discloses, teaches and suggests the use of a firewall at a fixed location which is utilized to control the access of client computers connected thereto.

In addition, the paragraph bridging pages 5 and 6 of the January 9, 2006 Response, wherein the use of a common first network address by each client computer without the use of a firewall is disclosed, clearly sets forth in the first sentence thereof that the limitations are not set forth in claim 1.

In the "Response to Arguments" section of the April 7, 2006 Office Action, the Examiner states:

> Regarding Applicant's argument that Stockwell does not teach communications between different network addresses, Examiner respectfully disagrees, noting Stockwell clearly teaches network communications via both static and dynamic IP addresses, (i.e.: DHCP – Col. 2, lines 47-67 & Col. 3, lines 1-4), which clearly and obviously reads upon communications between different network addresses. Further, as noted herein, within a system like that taught by Stockwell, three communication sessions would be an obvious number of communication sessions for a process involving initiation, authentication and redirection.

Column 2, line 47 through column 3, line 4 of the Stockwell et al. patent discloses the use of both static and dynamic IP addresses. However, nowhere does the Stockwell et al. patent disclose, teach or suggest the use of first, second and third communication sessions in the manner claimed in claim 1. In the foregoing quoted section of the April 7, 2006 Office Action, the Examiner attempts to trivialize the use of three communication sessions in the manner claimed in claim 1. However, the Examiner has not identified any teaching or suggestion in the prior art, nor has the Examiner explained why one skilled in the art would use three communication sessions versus any number of communication sessions other than three.

Claims 7 and 15:

In rejecting claims 7 and 15, the Examiner alleges, without evidence, that it would have been obvious to terminate communication sessions as new ones are created for reservation of bandwidth. Moreover, the Examiner alleges that column 5, line 17 through column 6, line 58;

column 7, line 34 through column 8, line 37; and column 11, line 6 through column 12, line 67 of the Stockwell et al. patent disclose the limitations of claims 7 and 15. However, a careful review of the Stockwell et al. patent reveals that these sections do not disclose, teach or suggest terminating either a first or second communication session established with a first or second network address by a client computer (the combination of claims 7 and 1, and claims 13 and 15). Moreover, as is noted above in connection with claim 1, the Stockwell et al. patent discloses, teaches and suggests inter process communications occurring within a firewall, not between different communication sessions with different network addresses.

Claim 10:

In rejecting claim 10, the Examiner alleges that the Stockwell et al. patent "further teaches including the step of transferring at least part of the conveyed data to the [second] network address via the [second] communication session." As noted above in connection with claim 1, however, the Stockwell et al. patent discloses, teaches and suggests inter process communications occurring within a firewall, not between different communication sessions at different network addresses. Moreover, nowhere does the Stockwell et al. patent disclose, teach or suggest transferring at least part of data conveyed via a third communication session with a third network address to a second network address via a second communication session (the combination of claims 10, 9 and 1).

Claim 13:

Independent claim 13 recites a method for controlling computer network access. The method includes: (a) storing at a client computer a first network address; (b) initiating a first communication session between the client computer and a first server computer at the first network address; (c) receiving at the client computer from the first server computer via the first communication session a second network address; (d) initiating a second communication session

between the client computer and a second server computer at the second network address; (e) receiving at the client computer from the second server computer an access configuration including a control setting for at least one communication protocol capable of being utilized during a third communication session; (f) instantiating on the client computer concurrent with the second communication session a process which initiates a third communication session between the client computer and a remote computer at a third network address; and (g) in connection with the third communication session, controlling data conveyed at least one of (i) to and (ii) from the instantiated process on the client computer based on the control setting for the one communication protocol.

For the reasons discussed above in connection with claim 1, the Stockwell et al. patent cannot render obvious claim 13. In addition, the Stockwell et al. patent does not disclose, teach or suggest the limitations of claim 13, step (f), namely, instantiating on the client computer concurrent with the second communication session (with a second server computer) a process which initiates a third communication session between the client computer and a remote computer at a third network address. Rather, as discussed above, the Stockwell et al. patent discloses, teaches and suggests communication sessions between internal processes of a firewall - not communication sessions with different network addresses.

Claims 8 and 18:

In rejecting claims 8 and 18, the Examiner alleges that "Stockwell clearly teaches a variable rule functionality wherein access to any number of multiple protocols would have been obvious to incorporate therein". Assuming *arguendo* the Examiner's allegation is correct, it does not meet the limitations of claims 8 and 18 wherein the client computer requests another access configuration via a second communication session with a second network address, receiving the other access configuration either from the second server computer (claim 18) or via the second

communication session (claim 8) and controlling data conveyed to or from the client computer based on a control setting including in the other access configuration.

Claim 22:

Independent claim 22 recites a method of controlling computer network access. The method includes: (a) initiating a communication session between a first computer and a second computer; (b) receiving at the first computer from the second computer via the communication session an access configuration including a control setting for at least one communication protocol; (c) monitoring data conveyed to or from a process running on the first computer based on the control setting; and (d) controlling the data conveyed to or from the process based on the control setting.

The Stockwell et al. patent does not disclose, teach or suggest the limitations of claim 22, step (b), namely, receiving at the first computer from the second computer via the communication session an access configuration including a control setting for at least one communication protocol. Rather, as discussed above, the Stockwell et al. patent discloses, teaches and suggests communications between internal processes of a firewall. In addition, the Stockwell et al. patent discloses, teaches and suggests that acld 60 (synonymous to the access configuration of the present invention) always resides at the firewall (see Stockwell et al. patent, column 7, lines 10-20).

CONCLUSION

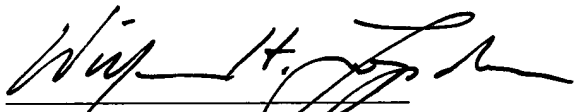
As can be seen, the Stockwell et al. patent does not disclose, teach or suggest a method having all the limitations of claims 1-23. Accordingly, the Stockwell et al. patent cannot render obvious claims 1-23 of the present application.

It is respectfully urged that the final rejection on the merits be reversed and a Notice of Allowance issued.

A check for $250 to cover the 37 C.F.R. § 41.20(b)(2) small entity fee for filing an Appeal Brief Under 37 C.F.R. § 41.37 accompanied the original Appeal Brief Under 37 C.F.R. § 41.37 mailed on September 7, 2006.

Respectfully submitted,

THE WEBB LAW FIRM

By 

William H. Logsdon
Registration No. 22,132
Attorney for Applicants
700 Koppers Building
436 Seventh Avenue
Pittsburgh, PA 15219
Telephone: 412-471-8815
Facsimile: 412-471-4094
E-Mail: webblaw@webblaw.com

(VIII) CLAIM APPENDIX

1. A method for controlling computer network access, the method comprising the steps of:

(a) initiating at a client computer a first communication session at a first network address;

(b) receiving at the client computer via the first communication session a second network address;

(c) initiating at the client computer a second communication session at the second network address;

(d) receiving at the client computer via the second communication session an access configuration including a control setting for at least one communication protocol capable of being utilized during a third communication session;

(e) instantiating on the client computer a process which initiates a third communication session at a third network address; and

(f) in connection with the third communication session, controlling the conveyance of data at least one of (i) to and (ii) from the process instantiated on the client computer based on the control setting for the one communication protocol.

2. The method as set forth in claim 1, wherein:

the access configuration includes a list related to the control setting for the one communication protocol; and

the conveyance of data via the third communication session is controlled based on the list.

3. The method as set forth in claim 1, wherein the one communication protocol includes one of:

World Wide Web (Web);

file transfer protocol (FTP);

E-mail;

News;

Chat;

Instant Messaging;

Telnet; and

Peer-to-Peer.

4. The method as set forth in claim 1, wherein the control setting is one of:

unrestricted computer network access (Allow All);

no computer network access (Block All);

limited computer network access to network addresses included in an allow list (Allow Listed); and

unrestricted computer network access except to network addresses included in a block list (Block Listed).

5. The method as set forth in claim 1, wherein:

the access configuration further includes at least one of the following global control settings:

access prohibited to conveyed data including a predetermined word or phrase;

access prohibited to data of at least one predetermined data type;

access prohibited to data conveyed during at least one of a predetermined time and day-of-week; and

access prohibited based on a rating for a category included with the conveyed data; and

step (f) further includes the step of controlling the conveyance of data at least one of (i) to and (ii) from the process instantiated on the client computer based on the at least one global control setting.

6. The method as set forth in claim 5, wherein the at least one predetermined data type includes an Internet cookie.

7. The method as set forth in claim 1, further including at least one of:

after step (b), the step of terminating the first communication session; and

after step (d), the step of terminating the second communication session.

8. The method as set forth in claim 1, further including the steps of:

transmitting from the client computer via the second communication session a request to receive another access configuration including a control setting for the one communication protocol;

receiving at the client computer via the second communication session the other access configuration; and

performing step (f) based on the control setting included in the other access configuration.

9. The method as set forth in claim 1, wherein step (f) further includes the steps of:

determining from the conveyed data the communication protocol thereof; and

determining from the thus determined communication protocol the control setting therefor.

10. The method as set forth in claim 9, further including the step of transferring at least part of the conveyed data to the second network address via the second communication session.

11. The method as set forth in claim 10, wherein the transferred data includes at least one of the following:

a network address; and

a subject of the third communication session.

12. The method as set forth in claim 10, further including the step of transferring with the data a login name received by the client computer during a login procedure by a user thereof.

13. A method for controlling computer network access comprising the steps of:

(a) storing at a client computer a first network address;

(b) initiating a first communication session between the client computer and a first server computer at the first network address;

(c) receiving at the client computer from the first server computer via the first communication session a second network address;

(d) initiating a second communication session between the client computer and a second server computer at the second network address;

(e) receiving at the client computer from the second server computer an access configuration including a control setting for at least one communication protocol capable of being utilized during a third communication session;

(f) instantiating on the client computer concurrent with the second communication session a process which initiates a third communication session between the client computer and a

remote computer at a third network address; and

(g) in connection with the third communication session, controlling data conveyed at least one of (i) to and (ii) from the instantiated process on the client computer based on the control setting for the one communication protocol.

14. The method as set forth in claim 13, wherein the first and second server computers are the same server computer.

15. The method as set forth in claim 13, further including at least one of:

after step (c), the step of terminating the first communication session; and

after step (e), terminating the second communication session.

16. The method as set forth in claim 13, wherein:

the access configuration further includes at least one of the following global control settings:

access prohibited to conveyed data including at least one of a predetermined word and a predetermined phrase;

access prohibited to data including at least one predetermined data type;

access prohibited to data conveyed during at least one of a predetermined time and day-of-week; and

access prohibited based on a rating for a category included with the computer data; and

step (g) further includes the step of controlling the conveyance of data at least one of (i) to and (ii) from the process instantiated on the client computer based on the at least one global control setting.

17. The method as set forth in claim 16, wherein:

prior to receipt of the access configuration at the client computer, the control setting for the one communication protocol is selected from a plurality of different control settings therefor; and

each global control setting is selected nonexclusively of any other global control settings.

18. The method as set forth in claim 13, further including the steps of:

initiating at the client computer via the second communication session a request to the second server computer to transmit another access configuration;

receiving at the client computer from the second server computer the other access configuration; and

performing step (g) based on a control setting included in the other access configuration for the one communication protocol.

19. The method as set forth in claim 13, wherein:

the access configuration includes for the control setting for the one communication protocol a list; and

the conveyance of data in step (g) is controlled based upon an entry included in the list.

20. The method as set forth in claim 19, wherein the entry comprises a network address.

21. The method as set forth in claim 13, further including the step of determining the communication protocol from the conveyed data.

22. A method of controlling computer network access comprising:

(a) initiating a communication session between a first computer and a second computer;

(b) receiving at the first computer from the second computer via the communication session an access configuration including a control setting for at least one communication protocol;

(c) monitoring data conveyed to or from a process running on the first computer based on the control setting; and

(d) controlling the data conveyed to or from the process based on the control setting.

23. The method of claim 22, wherein:

the process instantiates another communication session; and

the conveyance of data is controlled in connection with the other communication session.

(IX) EVIDENCE APPENDIX

NONE

(X) RELATED PROCEEDINGS APPENDIX

NONE